TCG Infrastructure Working Group Verification Result Schema

Specification Version 1.0
Revision 1.00
21 May 2007
Final

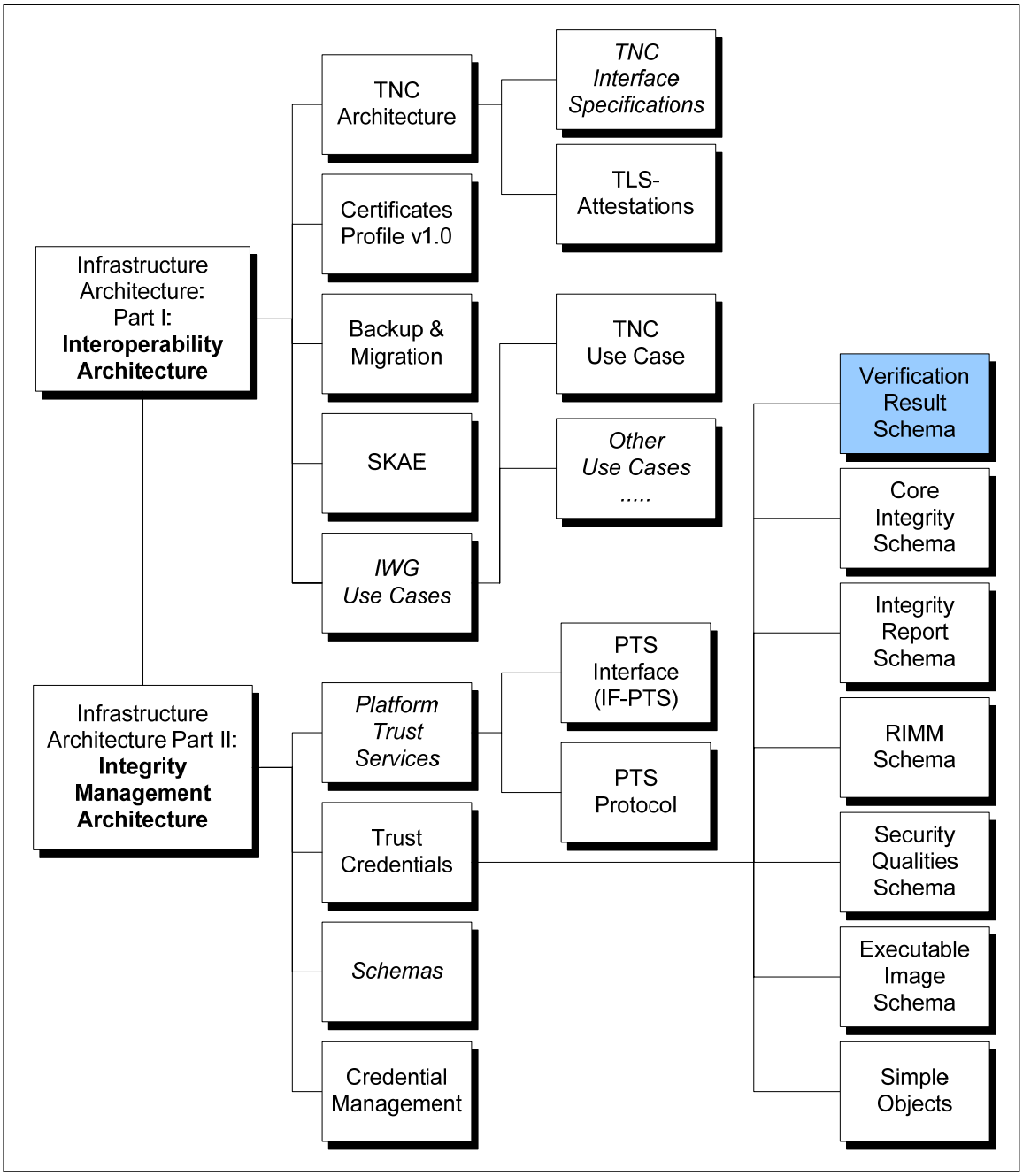
Contact: admin@trustedcomputinggroup.org

TCG

TCG PUBLISHED

Disclaimer

IWG Document Roadmap



Acknowledgement

The TCG wishes to thank all those who contributed to this specification. This document builds on considerable work done in the various working groups in the TCG.

Special thanks to the members of the IWG contributing to this document:

Name	Company
Malcolm Duncan	CESG
Mark Redman	Freescale Semiconductor
Diana Arroyo	IBM
Lee Terrell	IBM
Markus Gueller	Infineon
Ned Smith (IWG Co-Chair)	Intel Corporation
Wyllys Ingersoll	Sun Microsystems
Jeff Nisewanger	Sun Microsystems
Paul Sangster	Symantec
Thomas Hardjono (IWG Co-Chair)	Wave Systems
Greg Kazmierczak (Editor)	Wave Systems
Len Veil	Wave Systems

Table of Contents

1 Scope and Audience

This specification is integral to the TCG Infrastructure Working Group's (IWG) reference architecture, and is directly related to the TCG's Integrity Management Model. Specifically, the Verification Result XML schema defines the structure with which results of integrity measurement verifications are included within integrity reports.

Architects, designers, developers, and technologists interested in the development, deployment, and interoperation of trusted systems will find this document necessary in providing a specific mechanism for communicating integrity information.

2 Introduction

The purpose of this document is to provide a detailed description of the TCG Infrastructure Working Group's verification result XML schema, hereafter referred to as the *verification result schema*.

The verification result schema allows instantiation of interoperable snapshot and integrity report integrity measurement verification results. This schema is intended for use as a child of the Integrity Report Schema [9] and allows implementers to populate assertions of results of integrity measurement verifications. The primary use of this schema is to allow a Platform Trust Service (PTS) [8] to locally verify integrity measurements against Reference Manifests and XACML policies, and only report the results of the verifications to a relying party. This approach pre-processes the measurements and allows reporting of much smaller integrity reports containing the Reference Manifest and XACML policy evaluations instead of passing potentially voluminous raw measurement data. The schema may also be used to send verification results in addition to integrity measurements.

2.1 Normative Specification Content

The contents of this document should be considered to be NORMATIVE except for the XML schemas and associated structural diagrams. For XML schemas, the XML in this document is generated from the XSD files. While it is the intention of the authors to keep these representations consistent, the XSD files are considered NORMATIVE for all XML and any XML representations in this document are INFORMATIVE.

2.2 Schema Version

The report schema's version number is defined using the `version` attribute of the schema's root-level `schema` element:

```
version="version_number"
```

This document refers to version 1.0 of the verification result schema.

2.3 Schema Namespace

The verification result schema's namespace is defined using the `targetNamespace` attribute of the schema's root-level `schema` element:

```
targetNamespace="namespace"
```

The schema's namespace reflects the schema version, and is currently defined as follows:

```
http://www.trustedcomputinggroup.org/XML/SCHEMA/Verification_Result_v1_0#
```

2.4 Dependent Schema Definitions

2.4.1 W3C XML Schema Syntax

The simple object schema relies upon data structures defined by the World Wide Web Consortium's (W3C) XML-Schema syntax. Consequently, the simple object schema imports the W3C's XML schema with the following namespace:

```
http://www.w3.org/2001/XMLSchema
```

The report schema associates the abovementioned schema with the "xs" namespace prefix.

2.4.2 TCG Core Integrity Schema Syntax

The report schema relies upon data structures defined by the TCG Core Integrity Schema Syntax, [1]. Consequently, the report schema imports the TCG Core Integrity Schema with the following namespace:

```
http://www.trustedcomputinggroup.org/XML/SCHEMA/Core_Integrity_v1_0_1#
```

The report schema associates the abovementioned schema with the “core” namespace prefix.

2.5 Schema Diagram Conventions

The schema diagrams in this specification contain attributes and elements that are either mandatory or optional to populate. Those that are mandatory to populate are depicted by solid lines surrounding the attributes and elements. Those that are optional to populate are depicted by dashed lines surrounding the attributes and elements.

2.6 Keywords

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119 [11]. This specification does not distinguish blocks of informative comments and normative requirements. Therefore, for the sake of clarity, note that lower case instances of must, should, etc. do not indicate normative requirements.

2.7 Privacy Considerations

The results of evaluating rules and policies may expose privacy sensitive and personally identifiable information (PII). The verification result schema does not specifically require creation of privacy preserving rules and policies, however the SHOULD be created in compliance with the TCG Best Practices Guidelines. Rules and policies need to be evaluated on a case by case basis to determine whether they are PII friendly from the perspective of the platform owner or user.

3 Verification Result Schema

schema location: http://www.trustedcomputinggroup.org/XML/SCHEMA/Verification_Result_v1_0.xsd
attribute form default: Unqualified
element form default: Qualified
targetNamespace: http://www.trustedcomputinggroup.org/XML/SCHEMA/Verification_Result_v1_0#

3.1 COMPLEX TYPES

The following complex types are specified in this document:

Complex types
ResultType
VerifyResultType

Elements which are derived from these complex types are defined in section 3.2.

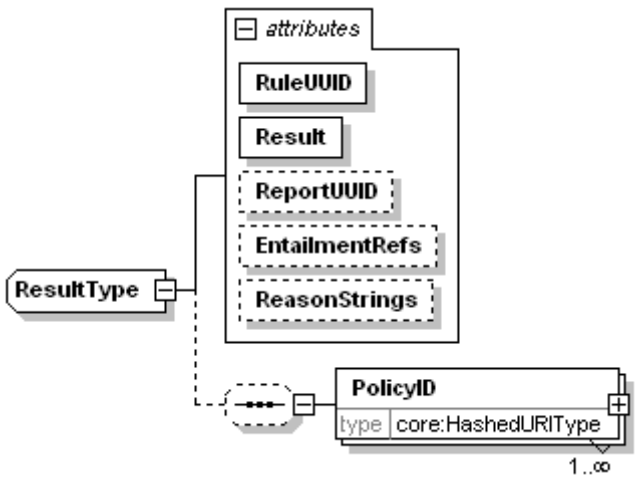
3.1.1 complexType ResultType

3.1.1.1 Description

The ResultType complex type represents the results of a single Reference Manifest or XACML rule verification. Included is information necessary to identify the Reference Manifest or XACML rule as well as the Integrity Report containing the original measurements and references to components that did not match expected values or policies. The PolicyHash element enables relying parties to detect if the document identified by PolicyID is identical to the version when this assertion was created. The support for multiple hash values was included to allow for multiple digest algorithms to be used in parallel (e.g. URI's content is digested both in SHA-1 and SHA-256.).

3.1.1.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Verification_Result_v1_0#

children **PolicyID**

used by element **VerifyResultType/Results**

attributes

Name	Type	Use	Default	Fixed
RuleUUID	xs:NMTOKEN	required		
Result	xs:NMTOKEN	required		
ReportUUID	xs:NMTOKEN	optional		
EntailmentRefs	xs:IDREFS	optional		
ReasonStrings	xs:NMTOKENS	optional		

3.1.1.3 Attribute Detail

Attribute	Description

RuleUUID	Document unique record instance identifier assigned by PTS of a Reference Manifest or an XACML policy. Reference Manifests and XACML policies as both called rules in IF-PTS [8].
Result	Result MUST be one of the following: VALID, INVALID, or UNVERIFIED. The UNVERIFIED result SHOULD be used when there was insufficient data to make a result decision or when the Reference Manifest (or XACML Policy) identified by RuleUUID (and PolicyID) could not be found or parsed.
ReportUUID	Universally unique identifier of the Integrity Report containing the integrity measurements used to evaluate RuleUUID.
EntailmentRefs	A list of document unique references within the Integrity Report referenced by ReportUUID that identify those components which caused the Result to be INVALID or UNVERIFIED. A verifier MAY use the combination of EntailmentRefs and ReportUUID to query PTS for integrity measurements of components that failed rule evaluation, if the measurement details are not already available to the verifier.
ReasonStrings	One or more strings that caused a verification result of INVALID or UNVERIFIED. This is particularly useful if an IDREF can not be used to reference a reason for the failed verification. Examples include: the transitive trust chain is missing or inadequately reported, a Quote is missing, confidence value is too low, etc.

3.1.1.4 XML

source

```
<xs:complexType name="ResultType">
  <xs:sequence minOccurs="0">
    <xs:element name="PolicyID" type="core:HashedURIType" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="RuleUUID" type="xs:NMTOKEN" use="required"/>
  <xs:attribute name="Result" use="required">
    <xs:simpleType>
      <xs:restriction base="xs:NMTOKEN">
        <xs:enumeration value="VALID"/>
        <xs:enumeration value="INVALID"/>
        <xs:enumeration value="UNVERIFIED"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
  <xs:attribute name="ReportUUID" type="xs:NMTOKEN" use="optional"/>
  <xs:attribute name="EntailmentRefs" type="xs:IDREFS" use="optional"/>
  <xs:attribute name="ReasonStrings" type="xs:NMTOKENS" use="optional"/>
</xs:complexType>
```

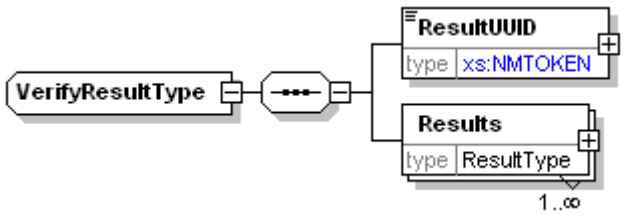
3.1.2 complexType VerifyResultType

3.1.2.1 Description

The VerifyResultType complex type represents the data returned from a single verification operation.

3.1.2.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Verification_Result_v1_0#

children **ResultUUID** **Results**

used by element **VerifyResult**

3.1.2.3 XML

source

```
<xs:complexType name="VerifyResultType">
  <xs:sequence>
    <xs:element name="ResultUUID">
      <xs:complexType>
```

```
        <xs:simpleContent>
          <xs:extension base="xs:NMTOKEN">
            <xs:attribute name="DependentResults" type="xs:NMTOKENS"/>
          </xs:extension>
        </xs:simpleContent>
      </xs:complexType>
    </xs:element>
    <xs:element name="Results" type="ResultType" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>
```

3.2 ELEMENTS

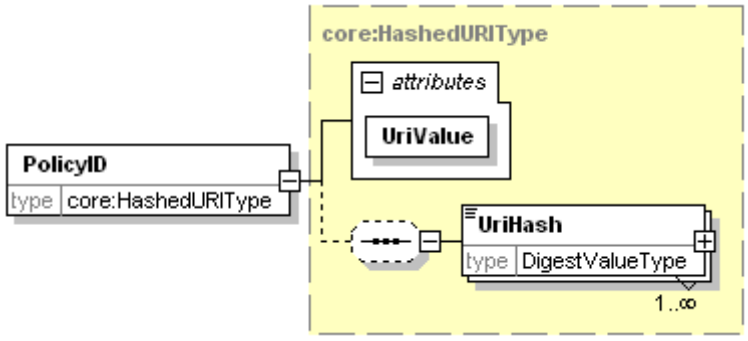
3.2.1 Element ResultType/PolicyID

3.2.1.1 Description

The PolicyHash element is an instance of core:HashedURIType (defined in [1]). This optional element contains as an attribute the URI of the XACML policy and optionally contains one or more hash values of the document found at the URI, thus enabling relying parties to detect if the document is identical to the version available when this assertion was created. The support for multiple hash values was included to support hash agility and allows for multiple digest algorithms to be used in parallel (e.g. URI's content is digested both in SHA-1 and SHA-256.).

3.2.1.2 Diagram

diagram



type	**core:HashedURIType**	
properties	isRef	0
	content	complex
children	**UriHash**	

attributes

Name	Type	Use	Default	Fixed
UriValue	xs:anyURI	required		

3.2.1.3 Attribute Detail

Attribute	Description
UriValue	The URI of an XACML policy if RuleUUID references an XACML policy and not a Reference Manifest. A verifier must check that the PolicyID is the correct one and map it to the RuleUUID.

3.2.1.4 XML

source

```
<xs:element name="PolicyID" type="core:HashedURIType" maxOccurs="unbounded"/>
```

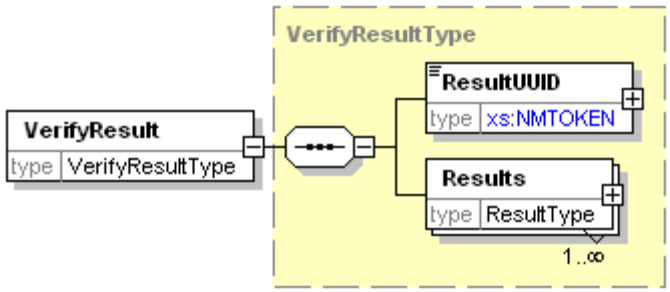
3.2.2 element VerifyResult

3.2.2.1 Description

The VerifyResult element is an instance of VerifyResultType (see section 3.1.2). This is a set of verification results from a single verification operation. VerifyResult is instantiated by the AssertionsInfo element in Snapshot (within an Integrity Report) [9] XML.

3.2.2.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Verification_Result_v1_0#

type **VerifyResultType**

properties content complex

children **ResultUUID** **Results**

3.2.2.3 XML

source

```
<xs:element name="VerifyResult" type="VerifyResultType"/>
```

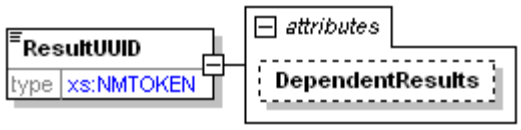
3.2.3 element VerifyResultType/ResultUUID

3.2.3.1 Description

The ResultUUID element is the universally unique identifier for the collection of results (i.e. for a single VerificationResult). ResultUUID extends the xs:NMTOKEN structure by adding a DependentResults attribute. DependentResults is a list of UUIDs (ResultUUIDs) of other VerificationResults which were used in the computation of this VerificationResult.

3.2.3.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Verification_Result_v1_0#

type extension of xs:NMTOKEN

properties isRef 0
content complex

attributes

Name	Type	Use	Default	Fixed
DependentResults	xs:NMTOKENS			

3.2.3.3 XML

source

```
<xs:element name="ResultUUID">
  <xs:complexType>
    <xs:simpleContent>
      <xs:extension base="xs:NMTOKEN">
        <xs:attribute name="DependentResults" type="xs:NMTOKENS"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
</xs:element>
```

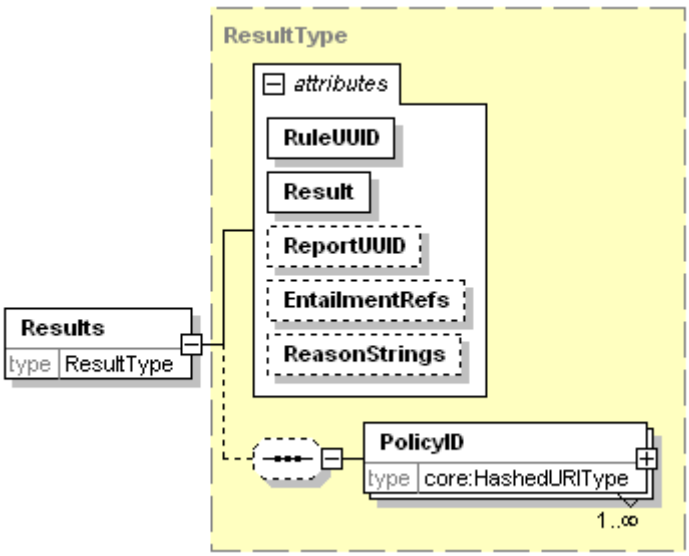
3.2.4 element VerifyResultType/Results

3.2.4.1 Description

The Results element is defined by the ResultType complex type (see Section 3.1.1).

3.2.4.2 Diagram

diagram



namespace http://www.trustedcomputinggroup.org/XML/SCHEMA/Verification_Result_v1_0#

type **ResultType**

properties
isRef 0
content complex

children **PolicyID**

attributes

Name	Type	Use	Default	Fixed
RuleUUID	xs:NMTOKEN	required		
Result	xs:NMTOKEN	required		
ReportUUID	xs:NMTOKEN	optional		
EntailmentRefs	xs:IDREFS	optional		
ReasonStrings	xs:NMTOKENS	optional		

3.2.4.3 XML

source

```
<xs:element name="Results" type="ResultType" maxOccurs="unbounded"/>
```

4 References

[1] Trusted Computing Group, TCG IWG Core Integrity Schema, Specification Version 1.0.1, Revision 1.0, 17 November 2006.

[2] Trusted Computing Group, TCG TPM Specification, TPM Main Part 2 TPM Structures, Specification version 1.2, Level 2, Revision 94, 17 November 2006.

[3] W3C, XML Schema, W3C Consortium, October 2004.

[4] Trusted Computing Group, TCG TPM Specification, TPM Main Part 3 Commands, Specification version 1.2, Level 2, Revision 94, 17 November 2006.

[5] Trusted Computing Group, TCG IWG Reference Manifest Schema, Specification Version 1.0, Revision 1.0, 17 November 2006.

[6] Trusted Computing Group, TCG IWG Architecture Part II, Specification Version 1.0, Revision 1.0, 17 November 2006.

[7] Trusted Computing Group, *TNC Architecture for Interoperability*, Specification Version 1.2, Revision 4, 21 May 2007.

[8] Trusted Computing Group, TCG Platform Trust Services Interface IF-PTS, Specification Version 1.0, Revision 1.0, 17 November 2006.

[9] Trusted Computing Group, TCG IWG Integrity Report Schema, Specification Version 1.0, Revision 1.0, 17 November 2006.

[10] Trusted Computing Group, TCG IWG Security Qualities Schema, Specification Version 1.1, Revision 7, 21 November 2006.

[11] Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels”, Internet Engineering Task Force RFC 2119, March 1997.